UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/912,403	07/26/2001	William Michael Raike	SMD-002	4247

51414 7590 12/11/2006

GOODWIN PROCTER LLP
PATENT ADMINISTRATOR
EXCHANGE PLACE
BOSTON, MA 02109-2881

EXAMINER	
NGUYEN, MINH DIEU T	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 12/11/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/912,403	RAIKE, WILLIAM MICHAEL	
	Examiner	Art Unit	
	Minh Dieu Nguyen	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 November 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *2-5,9,11 and 13-16* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *2-5, 9, 11, and 13-16* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on November 17, 2006 has been entered.

2. Claims 2-5, 9, 11 and 13-16 are pending.

Response to Arguments

3. Applicant's arguments with respect to claims 2-5, 9, 11 and 13-16 have been considered but are moot in view of the new ground(s) of rejection. Applicant argues that none of the cited references (i.e. Bleichenbacher) contemplates using packet-specific tags and a base key that are sent separately from the encoded data. The examiner respectfully disagrees, as cited in both claims 9 and 13, **only the key** is transmitted separate from the transmission of the encrypted data packets and the unique packet tags to a recipient, applicant also admitted that "specifically, Bleichenbacher describes a system which transmits a program identifier (i.e. not the key) with the encrypted programming content".

Claim Objections

4. Claims 3, 5, 9, 11 and 16 are objected to because of the following informalities:

a) As to claim 3, "...said base key..." should be "...said random base key...".

b) As to claims 5 and 16, "...from a group comprising SHA-1 and MD5..." should be "from the group consisting of SHA-1 and MD5...".

c) As to claim 9, "...based on the base key..." should be "...based on the random base key..." and "...encrypting the base key..." should be "...encrypting the random base key..."..

d) As to claim 11, "...the base key..." should be "...the random base key...".

Appropriate correction is required.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 4-5, 9, 11, 13 and 15-16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bleichenbacher et al. (6,735,313) in view of Gammie (5,029,207).

a) As to claim 9, Bleichenbacher discloses a method for securely transmitting streaming media (see Bleichenbacher, col. 1, lines 9-15) comprising: generating a random base key (e.g. master key, "m", see Bleichenbacher, col. 7, lines 20-23); encrypting the streaming media by creating different packet keys (e.g. program keys) for

each data packet (e.g. each transmitted program) of the streaming media and encrypting each data packet using the corresponding packet keys (i.e. each transmitted program is encrypted by the server using a program key, which is unique to the program, see Bleichenbacher, col. 4, line 66 to col. 5, line 1), the packet keys being based on the base key and unique packet tags (e.g. program identifier, "p", see Bleichenbacher, col. 2, lines 53-65) assigned to each data packet (i.e. a program key, K_p, is obtained by recursively applying one or more hash functions to the master key, "m", depending on the binary value of the program identifier, "p", see Bleichenbacher, col. 5, lines 50-53); transmitting the encrypted data packets and the unique packet tags to a recipient (see Bleichenbacher, col. 6, lines 6-8). Bleichenbacher is silent on the capability of encrypting the base key, thus creating an open key and transmitting the open key to a recipient in a transmission separate from the transmission of the encrypted data packets and the unique packet tags to a recipient. Gammie is relied on for the teaching of encrypting the base key (e.g. encrypting the key with a first secret serial number of the subscriber's replaceable security module, see Gammie, col. 8, lines 32-24), thus creating an open key and transmitting the open key to a recipient in a transmission separate from the transmission of the encrypted data packets and the unique packet tags to a recipient (i.e. the key may be sent over a separate data channel, see Gammie, col. 2, lines 10-12; Fig. 7, element 705; col. 12, lines 42-45). It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of encrypting the base key, thus creating an open key and transmitting the open key to a recipient in a transmission separate from the transmission of the

encrypted data packets and the unique packet tags to a recipient in the system of Bleichenbacher, as Gammie discloses, so as to securely protect and restrict access to transmitted multimedia information (see Bleichenbacher, col. 1, lines 9-12).

b) As to claim 4, Bleichenbacher, as modified above, discloses the method of claim 9 wherein said packet data is encrypted using a symmetric algorithm in conjunction with said packet keys (i.e. symmetric algorithm is the same algorithm with the same key is used for encryption and decryption, the program key, K_p, used to encrypt each transmitted program is based on a secure hash of the base key and unique packet tag, see Bleichenbacher, col. 5, lines 50-53, that same program key, K_p , is obtained to decrypt the received program, see Bleichenbacher, col. 6, lines 8-10).

c) As to claim 11, Bleichenbacher, as modified above, discloses the method of claim 9 wherein the packet keys are based on a secure hash of the base key and unique packet tags assigned to each data packet (i.e. a program key, K_p, is obtained by recursively applying one or more hash functions to the master key, "m", depending on the binary value of the program identifier, "p", see Bleichenbacher, col. 5, lines 50-53).

d) As to claim 5, Bleichenbacher, as modified above, discloses the method of claim 11 wherein the secure hash is based on a hash function selected from a group comprising SHA-1 and MD5 (see Bleichenbacher, col. 5, lines 43-47).

e) As to claim 13, the components of the limitations in this claim (i.e. receiving encrypted streaming media) are similar to those of claim 9 (i.e. transmitting streaming media), so the same rationale applied against claim 9 above.

Bleichenbacher discloses a method for receiving encrypted streaming media (see Bleichenbacher, col. 1, lines 9-15) comprising: receiving an encrypted packet stream, the packet stream comprising a plurality of packets, each packet comprising encrypted packet information and a unique tag value (see Bleichenbacher, col. 10, lines 15-17); extracting the unique tag value from each packet (see Bleichenbacher, col. 6, line 8); computing a unique packet key for each packet based on the unique tag value and the decrypted base key (see Bleichenbacher, col. 6, lines 9-16) and decrypting the packet information using the corresponding packet keys (see Bleichenbacher, col. 6, lines 9-10). Bleichenbacher is silent on the capability of receiving an encrypted base key in a transmission separate from the transmission of the encrypted packet stream and decrypting the base key (as Bleichenbacher is silent on the capability of encrypting the base key as addressed in the above claim 9). Gammie is relied on for the teaching of receiving an encrypted base key in a transmission separate from the transmission of the encrypted packet stream (i.e. the key may be sent over a separate data channel, see Gammie, col. 2, lines 10-12; Fig. 7, element 705; col. 12, lines 42-45) and decrypting the base key (see Gammie, col. 8, line 58 – col. 9, line 4). It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of receiving an encrypted base key in a transmission separate from the transmission of the encrypted packet stream and decrypting the base key in the system of Bleichenbacher as Gammie discloses so as to securely protect access to transmitted multimedia information (see Bleichenbacher, col. 1, lines 9-12).

f) As to claim 15, Bleichenbacherher, as modified above, discloses the method of claim 13 wherein the computation of the packet keys is based on a secure hash of the base key and unique packet tags assigned to each data packet (i.e. a program key, K_p, is obtained by recursively applying one or more hash functions to the master key, "m", depending on the binary value of the program identifier, "p", see Bleichenbacher, col. 5, lines 50-53).

g) As to claim 16, the limitation in this claim is similar to the one of claim 5, thus it is rejected with the same rationale applied against claim 5 above.

7. Claim 2 is rejected under 35 U.S.C. 103(a) as being unpatentable over Bleichenbacher et al. (6,735,313) in view of Gammie (5,029,207) and further in view of Hawthorne (5,768,381).

Bleichenbacher and Gammie disclose the recited method of claim 13, however they are silent in the capability of transmitting the open key by adding it to a header of the transmission. Hawthorne is relied on for the teaching of transmitting the open key (e.g. encrypted session key) by adding it to a header of the transmission (i.e. transmitting encrypted session key as header to the recipient, see Hawthorne, col. 1, lines 6-10). It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of transmitting the open key to the recipient by adding it to the stream header in the system of Bleichenbacher and Gammie, as Hawthorne teaches, so as to strengthen secure communications between two entities.

8. Claims 3 and 14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bleichenbacher et al. (6,735,313) in view of Gammie (5,029,207) and further in view of Stallings (Cryptography and Network Security).

a) As to claim 3, the combination of Bleichenbacher and Gammie discloses the claimed limitations of claim 9, in particular Gammie discloses encrypting the base key (e.g. encrypting the key with a first secret serial number of the subscriber's replaceable security module, see Gammie, col. 8, lines 32-24). However they are silent on the capability of the base key is encrypted using a public key encryption algorithm. Stalling is relies on for the teaching of the base key is encrypted using a public key encryption algorithm (i.e. either of the two related keys can be used for encryption, with the other used for decryption, see Stallings, pages 165-167). It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of having the base key encrypted using a public key encryption algorithm in the system of Bleichenbacher and Gammie, as Stallings discloses, so as to provide a different means or algorithm of encrypting transmitted information.

b) As to claim 14, the limitation in this claim is similar to the one of claim 3, thus it is rejected with the same rationale applied against claim 3 above.

Conclusion

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dieu Nguyen whose telephone number is 571-272-3873.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

mdh
12/7/06